(19) Canadian Intellectual Property Office
An Agency of Industry Canada

Office de la Propri,t, Intellectuelle du Canada
Un organisme d'Industrie Canada

(11) CA 2 395 381 (13) A1

(40) 21.06.2001
(43) 21.06.2001

(12)

(21) 2 395 381

(22) 15.12.2000

(51) Int. Cl.7: G06F 1/00

(85) 14.06.2002

(86) PCT/FR00/03550

(87) WO01/044949

(30) 99/15979 FR 17.12.1999

(71) ACTIVCARD,
24-28, avenue du G,n,ral-de-Gaulle
F-92156, SURESNES C□DEX, XX (FR).

(72) AUDEBERT, YVES (US).

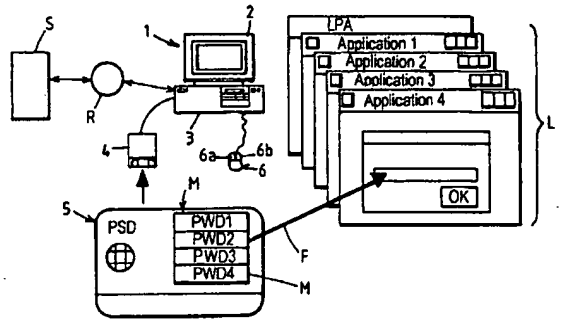
(74) FREEDMAN, GORDON

(54) DISPOSITIF INFORMATIQUE POUR L'APPLICATION DE DONNEES ACCREDITIVES A UN LOGICIEL OU A UN SERVICE

(54) COMPUTERISED DEVICE FOR ACCREDITING DATA APPLICATION TO A SOFTWARE OR A SERVICE

(57)

The invention concerns a device comprising data processing means, first storage means, interface means including at least a display screen (2), at least a pointing member for controlling the displacement of a cursor on said screen, and at least a software whereof the execution requires the application of at least one accrediting data in response to the display of a request on said screen. It further comprises a personal security device (5) comprising supply means (M) for delivering said accrediting data and means controlling access to said software including display means for simultaneously displaying on said screen said request (10) and at least a symbol (7) representing said personal security device (5), acquisition means (100) for controlling, by means of said pointing member, by positioning said cursor (9) on said symbol, the acquisition of said accrediting data in said supply means, and application means (122) for controlling, through said pointing member, said application of said data to said software in a required position of said cursor.



Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2395381 A1 2001/06/21

(21) 2 395 381

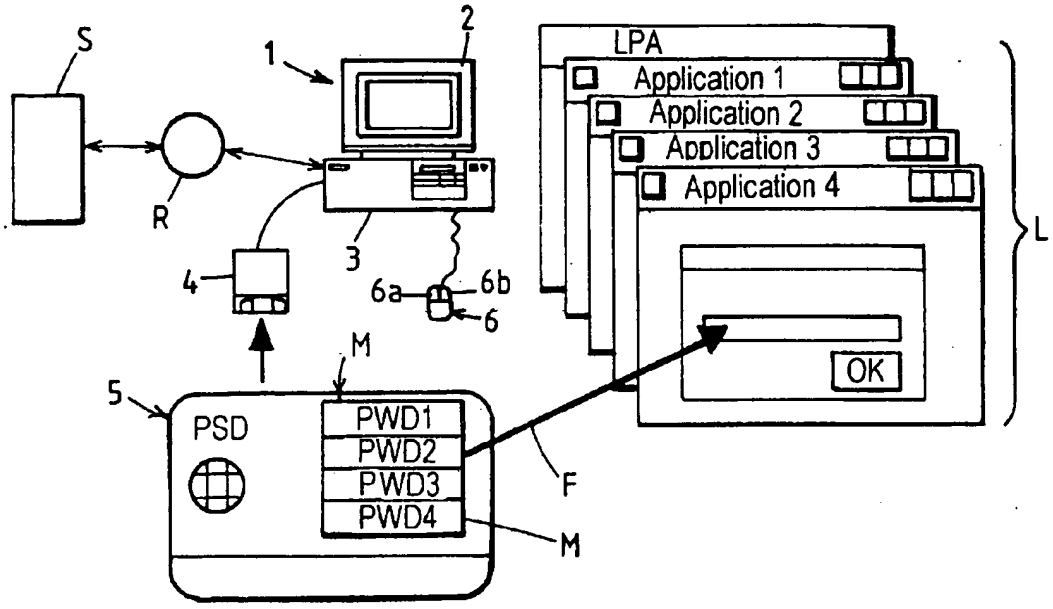
(12) DEMANDE DE BREVET CANADIEN
CANADIAN PATENT APPLICATION

(13) A1

(86) Date de dépôt PCT/PCT Filing Date: 2000/12/15
(87) Date publication PCT/PCT Publication Date: 2001/06/21
(85) Entrée phase nationale/National Entry: 2002/06/14
(86) N° demande PCT/PCT Application No.: FR 2000/003550
(87) N° publication PCT/PCT Publication No.: 2001/044949
(30) Priorité/Priority: 1999/12/17 (99/15979) FR

(51) Cl.Int.^{7}/Int.Cl.^{7} G06F 1/00
(71) Demandeur/Applicant:
ACTIVCARD, FR
(72) Inventeur/Inventor:
AUDEBERT, YVES, US
(74) Agent: FREEDMAN, GORDON

(54) Titre : DISPOSITIF INFORMATIQUE POUR L'APPLICATION DE DONNEES ACCREDITIVES A UN LOGICIEL OU A UN SERVICE
(54) Title: COMPUTERISED DEVICE FOR ACCREDITING DATA APPLICATION TO A SOFTWARE OR A SERVICE



(57) Abrégé/Abstract:
The invention concerns a device comprising data processing means, first storage means, interface means including at least a display screen (2), at least a pointing member for controlling the displacement of a cursor on said screen, and at least a software whereof the execution requires the application of at least one accrediting data in response to the display of a request on said screen. It further comprises a personal security device (5) comprising supply means (M) for delivering said accrediting data and means controlling access to said software including display means for simultaneously displaying on said screen said request (10) and at least a symbol (7) representing said personal security device (5), acquisition means (100) for controlling, by means of said pointing member, by positioning said cursor (9) on said symbol, the acquisition of said accrediting data in said supply means, and application means (122) for controlling, through said pointing member, said application of said data to said software in a required position of said cursor.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
21 juin 2001 (21.06.2001)

PCT

(10) Numéro de publication internationale
WO 01/44949 A3

(51) Classification internationale des brevets[7] : G06F 1/00

(21) Numéro de la demande internationale :
PCT/FR00/03550

(22) Date de dépôt international :
15 décembre 2000 (15.12.2000)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
99/15979 17 décembre 1999 (17.12.1999) FR

(71) Déposant : ACTIVCARD [FR/FR]; 24-28, avenue du Général de Gaulle, F-92156 Suresnes Cedex (FR).

(72) Inventeur: AUDEBERT, Yves; 237 Forrester Road, Los Gatos, CA 95032 (US).

(74) Mandataire : CABINET DE BOISSE ET COLAS; 37, avenue Franklin D. Roosevelt, F-75008 Paris (FR).

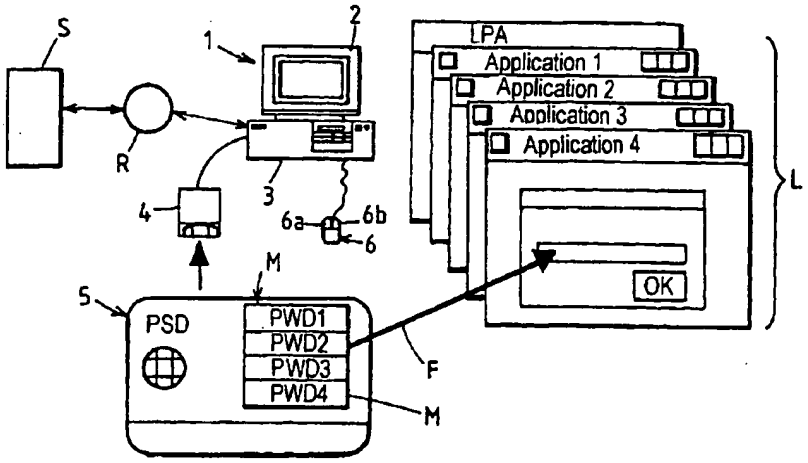
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU,

[Suite sur la page suivante]

(54) Title: COMPUTERISED DEVICE FOR ACCREDITING DATA APPLICATION TO A SOFTWARE OR A SERVICE

(54) Titre : DISPOSITIF INFORMATIQUE POUR L'APPLICATION DE DONNEES ACCREDITIVES A UN LOGICIEL OU A UN SERVICE



(57) Abstract: The invention concerns a device comprising data processing means, first storage means, interface means including at least a display screen (2), at least a pointing member for controlling the displacement of a cursor on said screen, and at least a software whereof the execution requires the application of at least one accrediting data in response to the display of a request on said screen. It further comprises a personal security device (5) comprising supply means (M) for delivering said accrediting data and means controlling access to said software including display means for simultaneously displaying on said screen said request (10) and at least a symbol (7) representing said personal security device (5), acquisition means (100) for controlling, by means of said pointing member, by positioning said cursor (9) on said symbol, the acquisition of said accrediting data in said supply means, and application means (122) for controlling, through said pointing member, said application of said data to said software in a required position of said cursor.

[Suite sur la page suivante]

WO 01/44949 A3

WO 01/44949 A3

MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*

(88) Date de publication du rapport de recherche internationale: 27 décembre 2001

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : Ce dispositif comprend des moyens de traitement de données, des premiers moyens de mémorisation, des moyens d'interface comportant au moins un écran d'affichage (2), au moins un organe de pointage pour commander le déplacement d'un curseur sur ledit écran, et au moins un logiciel dont l'exécution requiert l'application d'au moins une donnée accréditive en réponse à l'affichage d'une requête sur ledit écran. Il comprend en outre un dispositif de sécurité personnel (5) comportant des moyens de fourniture (M) pour la délivrance de ladite donnée accréditive et des moyens de pilotage d'accès audit logiciel comportant des moyens d'affichage pour afficher simultanément sur ledit écran ladite requête (10) et au moins un signe (7) représentatif dudit dispositif personnel de sécurité (5), des moyens d'acquisition (100) pour commander, au moyen dudit organe de pointage, par positionnement dudit curseur (9) sur ledit signe, l'acquisition de ladite donnée accréditive dans lesdits moyens de fourniture, et des moyens d'application (122) pour commander, au moyen dudit organe de pointage, ladite application de ladite donnée accréditive audit logiciel dans une position requise dudit curseur.

COMPUTERISED DEVICE FOR ACCREDITING DATA APPLICATION TO A SOFTWARE OR A SERVICE

The invention relates to a data processing system of the type in which the execution of a program or the access to a service or to a program is controlled by credentials specific to a user.

Access to many computer programs, such as operating systems and application programs, for example for electronic mail, e-commerce, home banking, etc, requires authentication of the user vis-à-vis the program concerned. When a user starts a program requiring authentication on a terminal such as a personal computer, the program generally displays on the screen of the terminal a dialog box including two fields, one for entering the login name of the user and the other for entering their password. These credentials are specific to the user and to the program concerned and the user enters them via the keyboard of the terminal.

Users usually use several application programs and therefore have to remember several login names and passwords. This constraint frequently leads users to write down their credentials, which compromises the security mechanisms implemented if the information written down is illegitimately discovered by a third party. Moreover, in order to be easily remembered by users, their passwords are generally short and offer only limited resistance to hacking.

The programs to which access requires authentication with which the present application is concerned can be programs which are either executed locally in a terminal such as a personal computer or executed partly in the terminal and partly in a server to which the terminal can be connected via a communication network such as the Internet. The programs concerned are primarily application programs for implementing operations of the type previously referred to (electronic mail, home banking, e-commerce, etc). In some cases the application programs enable execution of financial transactions and it is plainly essential to keep the credentials enabling access to them secret.

Using password servers to improve the security of the authentication process vis-à-vis applications is known in the art. Users wishing to access an application from a terminal must log on to the password server and authenticate themselves to the server. The password server, which contains the credentials of the user, is substituted for the user for the purpose of loading the required credentials into the application to which the user is

requesting access and starting the application. With this solution the credentials can remain unknown to the user, except for those enabling the user to authenticate themselves vis-à-vis the password server. However, this solution implies the existence of a dedicated server and requires a real time connection to the server when the user wishes to access an application.

Also, apart from questions related to access to programs as such, access to many services, for example for carrying out financial transactions or purchasing products via the Internet, requires the entry of data, secret or otherwise, such as a credit card number and expiry date, bank account number, etc. Entry of such data by a user via the keyboard or like device of a data processing system is a source of errors and complication and is prejudicial to security if the data is secret.

The invention aims to provide a data processing system significantly improving the ergonomics and the security of the process of applying credentials to a program or a service executed or to be executed by said system.

The invention also aims to provide a data processing system facilitating the process of authenticating a user vis-à-vis one or more programs or services to which access is controlled by credentials specific to the user and to the program or service concerned, avoiding the user having to remember the credentials associated with the program(s) or service(s) or to use a password server.

It further aims to provide a data processing system facilitating the application of payment data during telepurchasing operations by avoiding the user having to remember the number and expiry date of their payment card or the number of their bank account, for example.

Another object of the invention is to provide a data processing system which significantly improves the security of a process of the above kind of applying credentials to a program or a service.

To this end, the invention provides a data processing system including:

- data processing means for implementing at least one of the following functions: access to a program, execution of a program and access to a service,
- first means for storing data and programs,
- user interface means including at least one display screen and graphical interface means, and

- at least one pointing device for controlling the movement of a cursor over said screen,

- in which system implementing said function requires the application of credentials in response to the display of a request on said screen,

characterized in that it further includes a personal security device including supply means for delivering said credentials and means for controlling access to said program and including:

- display means for simultaneously displaying on said screen said request and at least one sign representing the personal security device,

- acquisition means for commanding the acquisition of said credentials in said supply means by positioning said cursor on said sign by means of said pointing device, and

- application means for commanding said application of said credentials to said function in a required position of said cursor, by means of said pointing device.

The data processing system according to the invention does not require manual entry by the user of their credentials, which are automatically transferred by means of the pointing device of the personal safety device to the software to which the user requires access. Because the user's personal security device, whether of the hardware type (smart card, token) or the software type, can store strong (long and complex) passwords, the data processing system according to the invention significantly improves security for access to one or more programs.

The growth of applications and services accessible via the Internet has indirectly created a proliferation of viruses, one objective of which is to read passwords or credit card numbers stored by users on their personal computer (PC) to avoid having to enter them each time they are used. The system according to the invention therefore improves security in that said credentials are protected by the user's personal security device and consequently are not stored in clear on the PC.

No real time connection to a password server containing the credentials of a set of users is necessary because the credentials specific to each user are stored in their personal security device, which is associated with the terminal from which the user requests access to an application. However, if a password server of the above kind exists, the data processing system according to the invention can be used to improve the security of the process of authentication vis-à-vis that server: the credentials controlling access to the

server are then managed in the manner described above.

The credentials referred to can be static passwords or dynamic passwords. In the case of static credentials, the means supplying said credentials are in fact memory means. In the case of dynamic credentials, the means supplying the credentials are computation means for executing an algorithm. The dynamic credentials are computed with the aid of time variables of the "event counter" type, a key, which itself is static or dynamic, and an algorithm executed in the smart card or the hardware or software token.

According to one feature of the invention, when said program is of the windows type and includes a destination window for said application of said credentials, said access control means further include:

- first means for identifying characteristic data of the window under said cursor while it is moving on said screen,
- first comparator means for comparing the characteristic data of said window under the cursor with characteristic data of said destination window stored in said supply means related to said credentials, and
- means for authorizing said application of said credentials in response to a match between said identified characteristic data and said characteristic data stored in said supply means.

In one embodiment of the invention, if the system includes a plurality of programs and a plurality of separate credentials controlling access to respective programs, each of the credentials is associated in said supply means with data identifying the corresponding program, said display means are adapted to display on said screen a plurality of signs respectively representing said credentials, and said access control means further include second means for identifying a program whose destination window is displayed on said screen, and second comparator means for comparing the identity of said identified program with identification data associated with credentials selected by means of said pointing device, said comparator means authorizing application of the selected credentials to said identified program only if said identified program and said identification data are identical.

In a variant of the invention, if the system includes a plurality of programs and a plurality of separate credentials controlling access to respective programs, each of the credentials is associated in said supply means with data identifying the corresponding program, and said access control means further include second means for identifying a program whose

destination window is displayed on said screen, and second comparator means for comparing the identity of said program detected with said identification data stored in said supply means, said application means being adapted to command application in said destination window of credentials present in said supply means and whose associated identification data corresponds to the identity of said detected program. In this embodiment the authentication process is automated in the sense that the user does not have to choose the credentials assigned to the program to which access is required, provided that the credentials are available in the personal security device.

The system preferably includes means for authorizing entry of credentials for said detected program by said user via said interface means and storing of said credentials entered with identification data of said detected program in said supply means if there is no match between said identification data and said detected program.

The data processing system according to the invention preferably further includes one or more of the following features separately or in combination:

- it includes a personal computer to which said personal security device is connected;
- said program is an application program divided between the personal computer and a server and said system includes means for connecting said personal computer to said server;
- said personal security device is a smart card;
- said personal security device includes means for comparing a stored secret code with a secret code entered by the user via said interface means and said access control means are rendered operational in response to a match between said secret codes; and
- said access control means include means for preventing display of said credentials on said display screen in response to their application to said program.

Thanks to this last feature in particular, the authentication process can be implemented without the user knowing their credentials, which significantly improves security because the user cannot inadvertently divulge the credentials.

If the credentials are static, the means supplying the credentials are memory means. If the credentials are dynamic, the means supplying the credentials include means for executing an algorithm for computing said

credentials.

Other features and advantages of the invention will emerge from the following description, which is given with reference to the accompanying drawings, in which:

Figure 1 is a diagrammatic view of the hardware and software elements of a data processing system according to the invention;

Figure 2A shows a display screen illustrating the process of authentication vis-à-vis a program by means of the system according to the invention;

Figure 2B is a view to a larger scale of an icon displayed on the screen shown in Figure 2A;

Figure 3 is a flowchart showing the basic functions implemented by a "Drag-and-Drop" application used in the system according to the invention;

Figure 4 is a more detailed flowchart showing a first subroutine of the software whose flowchart is shown in Figure 3;

Figure 5 is a more detailed flowchart showing a second subroutine of the software whose flowchart is shown in Figure 3;

Figure 6 is a diagrammatic representation of a home page of an application program displayed to a user so that they can enter their password.

Referring to Figure 1, a personal computer 1 includes a display screen 2 and a conventional set of means 3 for processing data (microprocessor), storing data, input/output of data, etc. To simplify the diagram the keyboard of the personal computer 1 is not shown.

The personal computer 1 is associated with a personal security device PSD such as a smart card 5 that can be read by a reader 4 connected to the personal computer 1. The reader can instead be integrated into the personal computer 1.

A pointing device, such as a mouse 6 with left-hand and right-hand buttons 6a, 6b, is conventionally connected to the personal computer 1 for moving a cursor on the screen 2.

The personal computer 1 is adapted to execute a number of programs L, in particular application programs illustrated in Figure 1 by a home page carrying the name of the application, namely Application 1, Application 2, Application 3 and Application 4, together with an access control program LPA managing access to the application programs (see below). The application programs (also referred to as applications hereinafter) can be executed locally in the personal computer 1 or executed partly in the personal computer and

partly in a server S to which the personal computer 1 can be connected via a communication network R such as the Internet, in a client-server architecture.

Access of a user of the personal computer 1 to any of the applications 1, 2, 3 and 4 is conditional on the entry of credentials which are assigned to the user to authorize the user to use the application concerned. The credentials generally include a login name and a password which are specific to the application and to the user concerned. Hereinafter, to simplify the description, only the credentials consisting of the password PWD will be considered. Thus passwords PWD1, PWD2, PWD3, PWD4 must be entered into the personal computer 1 to access the respective applications 1, 2, 3 and 4.

In a conventional system the user is prompted by a dialog box to enter their password at the keyboard and the characters typed are shown in clear or in some non-specific form (for example as a series of asterisks) in a specific window.

In a system according to the invention, the various credentials, and in particular the passwords PWD1, PWD2, PWD3, PWD4 for the applications 1 to 4, are supplied to the personal computer 1 by the personal security device 5. As previously indicated, the credentials, such as the passwords, can be static or dynamic.

In the sense of the present application, a personal security device PSD is a device held exclusively by or accessible exclusively to (for example by means of a personal identification code PIN or otherwise) an authorized user, and enabling secure storage therein of data with guaranteed security against reading and/or writing of data by unauthorized persons. Furthermore, a personal security device PSD of the above kind can include computing means for executing one or more algorithms, in particular algorithms for generating dynamic credentials.

As is the case in the embodiments described, the personal security device PSD can be a smart card 5, which can be connected to the personal computer 1 via the reader 4 and is provided with hardware and software security means enabling storage therein of secret data (codes, messages, keys, programs, etc). Its use is generally conditional on the provision of a personal identification code PIN. A smart card generally has no electrical power supply and its electronic circuits can be activated only by inserting it into a reader which can supply it with electrical power.

Other personal security devices which are well known in the art and

based on somewhat different security mechanisms do have an integral electrical power supply and can be used for authentication vis-à-vis a personal computer, a data processing system, etc. These personal security devices, which are generally portable, are also referred to as "tokens".

The personal security device PSD can instead take the form of software installed on the personal computer 1 and enabling secure storage therein of data, which data can optionally be encrypted.

It must be understood that the invention described in this application is not limited to the use of a smart card 5 as a personal security device, and that the personal security device could equally well be a "token" able to communicate with the personal computer 1 via bidirectional transmission means, a personal security device entirely in the form of software installed on the personal computer 1, or any other device specific to a user (access to which is generally controlled by a personal identification code PIN known to the user) for storing secret data in a secure manner and possibly for executing computation algorithms in the case of dynamic credentials.

The credentials, or the secret data for computing them in the case of dynamic passwords, are stored in segments of a memory M of the personal security device and their number is limited only by the memory of the device. Other limitations may relate to the capacity of the device PSD to execute computation algorithms.

Hereinafter, to simplify the description, the personal security device considered is a smart card 5 and the passwords PWD1, PWD2, PWD3, PWD4 supplied by it are static (stored) passwords or dynamic (computed) passwords.

The passwords PWD1, PWD2, PWD3, PWD4 supplied by the smart card 5 are associated with the features of the window in which the passwords are entered, in this instance the class and the attributes of the window.

The process illustrated by the dashed line arrow F in Figure 1 for entering the password supplied by the smart card 5 into the required window of one of the applications 1 to 4 will be explained further with reference also to Figures 2A and 2B.

The process is based on the use of graphical user interface "Drag-and-Drop" type functions. The Drag-and-Drop technique is a graphical user interface (GUI) technique for transferring data between two applications. The mouse of the personal computer is used to extract data from one application and insert it into another application. For example, it is possible to select a

block of text in a word processing program. Moving the cursor onto the selected block of text with the mouse and holding down the mouse button while moving the mouse to shift the cursor to the required location in another application inserts the text into that other application simply by releasing the mouse button. The Drag-and-Drop technique therefore presupposes a source, namely an application from which data is extracted, and a target, into which the data is inserted.

In the system according to the invention the source is the access control program LPA adapted to display at all times an icon 7 taking the form of a representation of a smart card, for example as shown in Figure 2B. The icon 7 is displayed and accessible at all times on the display screen 2, for example in the bottom right-hand corner of the screen, because the access control program LPA is a resident application, i.e. an application that executes continuously in the background and is started automatically each time that the user boots up the personal computer 1.

The target is the window 8 for inserting the password of the home page of the application to which access is required. Most modern application programs for personal computers with a windows type graphical user interface have a dialogue box with fields or windows enabling the user to enter their credentials. However, the system according to the invention is not limited to this type of application and can be used with older application programs that function without windows, in text mode, and simply prompt the user to enter their credentials.

When the user wishes to connect to one of the applications 1 to 4, for example application 1 as shown in Figure 2A, they move the cursor 9 onto the icon 7 using the mouse 6.

In a first embodiment of the invention, the user chooses from a menu the password PWD1, PWD2, PWD3 or PWD4 which corresponds to the displayed application. It must be understood that the passwords PWD1, PWD2, PWD3, PWD4 are not shown in clear in the menu and that only codes, messages or signals P1, P2, P3, P4 appear in the menu to enable them to be identified and to indicate to which application each of them provides access.

For example, briefly depressing the right-hand mouse button 6b when the cursor 9 is over the icon 7 calls up a list of password identification codes P1, P2, P3, P4. The required password, for example PWD1, is selected by placing the cursor 9 on the corresponding code P1 in the list and clicking the right-hand mouse button 6b, after which the icon 7 is displayed again. The

password PWD1 is thereafter selected by default and used automatically during subsequent "Drag-and-Drop" authentication processes until the user selects a different password from the menu.

When a password has been selected, with the cursor 9 over the icon 7, the user depresses the left-hand mouse button 6a and, while holding that button down, moves the cursor 9 by means of the mouse 6 toward the destination window 8. During this movement and until the cursor 9 reaches the destination window the access control software LPA modifies the graphical representation of the cursor: as shown in Figure 2A, while it is moving to the window 8 the cursor 9 takes the form of a circle with a diametral bar. When the cursor 9 reaches the destination window 8, it reverts to its original arrow shape, which tells the user that they can release the left-hand button 6a of the mouse 6.

As described hereinafter with reference to Figures 3 and 4, this modification of the graphical representation of the cursor 9 is managed by the access control program LPA which, while the cursor 9 is moving, continuously compares the class of the window under the cursor with the class of the destination window, whose characteristics are associated with the selected password PWD in the smart card 5. Releasing the left-hand button 6a of the mouse 6 when the cursor 9 reaches the window 8 commands insertion into the destination window 8 of the password PWD supplied by the smart card 5.

The above is merely an example, of course, and from an ergonomic point of view there are many other ways of inserting a password selected by a user from a set of identification codes representing different passwords into a destination window using a pointing device.

It must be understood that the applications 1, 2, 3 and 4 are not modified in any way and are standard applications. Consequently, the resident access control program LPA is substituted for entry of the password via the keyboard by the user. Various solutions for this are available to the skilled person. One solution is to simulate the pressing of the keyboard keys and to send to the destination window a message equivalent to that generated by the keyboard. With this solution, the password is transmitted character by character to the destination window. Another solution would be to use the cut/paste function offered by modern operating systems (OS): the password is copied onto the clipboard by the program LPA which then simulates pasting into the target application by sending it a message equivalent to the paste instruction. Finally, the program LPA erases the content of the clipboard to

avoid leaving the password exposed.

It follows from the foregoing description that the password PWD transmitted from the smart card 5 by means of the access control program LPA appears in the destination window 8 in the same form as if the user had typed it on the keyboard. This means that if the application is designed to display the password in clear it will remain displayed in clear in the destination window 8. However, even in this case security is improved because the display of the password PWD is transient and, in the case of a static password, the user does not need to memorize it or take the risk of writing it down.

However, in many cases, application programs are designed to display dummy characters, for example asterisks, instead of the characters of the password typed by a user: in this case, the password will never appear in clear and may even be totally unknown to the user, for example if the password PWD is loaded directly into their smart card by a personalizing tool under the control of a security administrator.

If the password used is a static password it can be strong, i.e. long and complex (for example a series of random characters), which in practice is not possible with the conventional solution requiring the user to memorize it.

In order further to strengthen the security of the authentication process vis-à-vis an application to which access is controlled by a password, the password can be dynamic rather than static. Dynamic passwords can be asynchronous or synchronous. This is known in the art.

An asynchronous password presupposes that the application and the personal security device share a secret key. The application generates a challenge that is transmitted to the personal security device PSD. The device encrypts the challenge using the secret key stored in its memory and an encryption algorithm, and the password computed in this way is transmitted to the application. The application carries out in parallel a similar calculation on the challenge and compares the result obtained with the password received from the personal security device. Access to the application is authorized if the passwords calculated in the application and in the PSD match, for example if they are identical.

Provided that the access control software LPA is in a position to read the challenge generated by the application, the system according to the invention enables the use of an authentication mechanism using asynchronous passwords of the above kind by having the access control

software, after reading the challenge, transmit it to the personal security device PSD and then, as previously described, the computed password inserted into the destination window.

Synchronous passwords vary in time, preferably each time they are used, for example in accordance with a timebase and/or an event counter. The passwords, or the keys and variables used to compute them, evolve synchronously in the personal security device PSD and in the application. These mechanisms are well known to the skilled person and are not described in more detail here. However, international patent application WO 99/18546, filed 1st October 1998, describes mechanisms for implementing authentication by a dynamic password based on time and using a smart card, despite the absence of an electrical power supply and consequently of a clock in a card of this kind.

In the embodiment shown in Figures 2A and 2B it is assumed that the user uses the cursor 9 to choose from a menu the code corresponding to the password PWD for the application they wish to access.

The following description with reference to Figures 3 to 6 covers a second embodiment in which the user does not need to select the appropriate password, because it is selected automatically by the access control program LPA.

Figure 3 shows the overall way in which the mouse 6 controls the access control program LPA. The process starts with step 100 in which the left-hand mouse button 6a is pressed when the cursor 9 is on top of the icon 7. Step 101 corresponds to capture of the status of the mouse and step 102 to waiting for events that can be generated by the mouse, for example moving the mouse or releasing the left-hand mouse button.

If the event detected is movement of the mouse, the next step is step 103 corresponding to the subroutine whose flowchart is shown in Figure 4.

If the event detected by the access control software concerns the left-hand mouse button, the next step is step 104 corresponding to the subroutine whose flowchart is shown in Figure 5. Step 105 is the last step of the main program.

The Figure 4 subroutine starts in step 106 with detection of movement of the mouse. In step 107 the position of the mouse is acquired. In step 108 the window under the cursor 9 is sought. Step 109 corresponds to the acquisition of characteristic data of the window under the cursor, in particular its class.

Step 110 determines if the class of the window under the cursor corresponds to a window class stored in the smart card 5. If not, the graphical representation of the cursor 9 is modified in step 111 to advise the user that at this stage the function for entering the password PWD is inhibited, i.e. that releasing the left-hand mouse button 6a will have no effect. The next step of the subroutine is then the end step 112. However, the Figure 4 subroutine is repeated for as long as the mouse 6 is moving, as is clear from the Figure 3 flowchart.

If the result of the test in step 110 is positive, i.e. if the window under the cursor is of a class contained in the memory of the smart card 5, step 113 modifies the graphical appearance of the cursor (which reverts to the arrow shape that it has when it reaches the window 8 in Figure 2), advising the user that insertion of the password PWD is then authorized.

If the event detected in step 102 in Figure 3 is releasing the left-hand mouse button, the subroutine 104 shown by the Figure 5 flowchart is executed.

Step 114 in Figure 5 corresponds to detecting release of the left-hand mouse button. The position of the mouse is acquired in step 115 and the window under the cursor is sought in step 116. Characteristic data of that window, in particular its class, is acquired in step 117.

Step 118 applies a test to determine if the window under the cursor 9 belongs to a class stored in the smart card 5. If not, the subroutine terminates in step 119.

If it does, the application to which the window belongs is determined in step 120. Step 121 applies a test to determine if the identified application corresponds to an application whose identification data is contained in the smart card 5. If it does, the password in the smart card 5 associated with the identified application is inserted in the window in which the cursor is then located, after which the subroutine terminates in step 123.

If the result of the test in step 121 is negative, the user is prompted in step 124 to enter the required password (static password) manually via the keyboard of their personal computer. In step 125 the password, the application identification data and the characteristics of the detected window acquired in steps 117 and 120 are transmitted to the smart card 5, which stores them. The next step of the subroutine is then step 122 which inserts the password entered at the keyboard by the user and stored in the smart card 5 into the destination window.

Figure 6 is a diagrammatic representation of a home page of an application and is used to explain the information collected during execution of the Figure 4 and 5 subroutines.

In a home page like the home page shown here, there is generally a data entry field in the destination window 8 into which the password PWD must be inserted. The window is characterized by its class and its specific attributes, for example an attribute characteristic of a password window.

The destination window is in a dialogue box 10. The dialogue box is characterized in particular by the title of the window, shown in the title bar of the dialog box, for example in the form "Enter password".

Finally, the main window of the application, i.e. the window of the target application, is characterized in particular by the class of the window and by the title 11 of the window. The title is generally formed by concatenating the name of the application and the name of the document open in the application, for example the file name of a text file or the address of a web page.

In steps 109, 117 or 120 of the Figure 4 and 5 subroutines the above information is used as previously described to determine if the insertion of a password is authorized or not.

If access to an application is conditional on the provision of several credentials, for example the user name (login name) and a password, the access control software LPA is adapted:

- to determine if the destination window in which the user released the button of the mouse 6 is that which is to receive the login name or that which is to receive the password; and

- looks for another adjoining window of the same dialog box that will receive the login name or the password, depending on the result of the preceding step.

The discrimination between login name and password windows is performed by examining if the window concerned has the "password" attribute, i.e. if the window is adapted to conceal what is entered by means of asterisks.

The second window is looked for by seeking the parent of the first window and then listing all the daughter windows of that parent until a window is found having the required characteristics. However, in some cases this solution may not work (dialog box with more than two entry windows, "password" attribute not used, etc.).

Another solution consists of having the user perform an initialization:

at the time of the first "drop" in an "unknown" dialog box of an application, the program LPA guides the user as to what to do next, i.e. it shows the user a facsimile of the target dialog box with its entry windows, the list of passwords (in the form of their codes P1, P2, etc) and login names already present in the card, and the possibility of adding new ones.

The user makes the link between the passwords and the login names by indicating which credentials (login name or password) must be inserted into the window, for example using the mouse. All this information is stored in the smart card for subsequent re-use at the time of requests for authentication vis-à-vis the application concerned.

It goes without saying that the embodiments described are merely examples of the invention and that they can be modified, in particular by substituting technical equivalents, without departing from the scope of the invention.

For example, in the case of a static password, the password can be stored in the memory M of the personal security device PSD in encrypted form and/or in the form of secret data for calculating the password as such. In this case, the personal security device PSD includes means for executing one or more algorithms for calculating the static password that will be supplied to the personal computer.

On the other hand, the system described above can also be applied to entry of data, such as credit card number and expiry date, bank card number, etc, needed to access a service or program, or to execute a program, whether or not access thereto is controlled by the entry of access credentials (password, login name, etc).

CLAIMS

1. A data processing system including:

- data processing means for implementing at least one of the following functions: access to a program, execution of a program and access to a service,

- first means for storing data and programs,

- user interface means including at least one display screen and graphical interface means, and

- at least one pointing device for controlling the movement of a cursor over said screen,

- in which system implementing said function requires the application of credentials in response to the display of a request on said screen,

characterized in that it further includes a personal security device (5) including supply means (M) for delivering said credentials and means (LPA) for controlling access to said program and including:

- display means for simultaneously displaying on said screen said request (10) and at least one sign (7) representing the personal security device (5),

- acquisition means (100) for commanding the acquisition of said credentials in said supply means (M) by positioning said cursor (9) on said sign by means of said pointing device (6), and

- application means (122) for commanding said application of said credentials to said function in a required position of said cursor, by means of said pointing device.

2. A system according to claim 1, wherein said program is of the windows type and includes a destination window (8) for said application of said credentials, characterized in that said access control means further include:

- first means (109, 117) for identifying characteristic data of the window under said cursor (9) while it is moving on said screen,

- first comparator means (110, 118) for comparing the characteristic data of said window under the cursor with characteristic data of said destination window (8) stored in said supply means (M) related to said credentials, and

- means (113) for authorizing said application of said credentials in response to a match between said identified characteristic data and said characteristic data stored in said supply means (M).

3. A system according to claim 2, characterized in that it includes a plurality of programs and a plurality of separate credentials (PWD1, PWD2, etc) controlling access to respective programs, each of the credentials is associated in said supply means with data identifying the corresponding program (Application 1, etc.), said display means are adapted to display on said screen a plurality of signs (P1, P2, etc) respectively representing said credentials, and said access control means further include:

- second means (120) for identifying a program whose destination window (8) is displayed on said screen, and
- second comparator means (121) for comparing the identity of said identified program with identification data associated with credentials selected by means of said pointing device, said comparator means authorizing application of the selected credentials to said identified program only if said identified program and said identification data are identical.

4. A device according to claim 2, characterized in that it includes a plurality of programs and a plurality of separate credentials (PWD1, PWD2, etc) controlling access to respective programs, each of the credentials is associated in said supply means with data identifying the corresponding program (Application 1, etc), and said access control means further include:

- second means (120) for identifying a program whose destination window (7) is displayed on said screen, and
- second comparator means (121) for comparing the identity of said program detected with said identification data stored in said supply means (M),
- said application means (121) being adapted to command application in said destination window of credentials present in said supply means (M) and whose associated identification data corresponds to the identity of said detected program.

5. A system according to claim 4, characterized in that it includes means (124, 125) for authorizing entry of credentials for said detected program by said user via said interface means and storing of said credentials entered with identification data of said detected program in said supply means if there is no match between said identification data and said detected program.

6. A system according to any of claims 1 to 5, characterized in that it includes a personal computer (1) to which said personal security device (5) is connected.

7. A system according to claim 6, characterized in that said program (Application 1, etc) is an application program divided between the personal computer and a server and said system includes means for connecting said personal computer to said server.

8. A system according to any of claims 1 to 7, characterized in that said personal security device is a smart card (5).

9. A system according to any of claims 1 to 8, characterized in that said personal security device (5) includes means for comparing a stored secret code (PIN) with a secret code entered by the user via said interface means and said access control means are rendered operational in response to a match between said secret codes.

10. A system according to any of claims 1 to 9, characterized in that said access control means include means for preventing display of said credentials on said display screen in response to their application to said program.

11. A system according to any of claims 1 to 10 wherein said credentials are static, characterized in that said supply means (M) are memory means.

12. A system according to any of claims 1 to 11 wherein said credentials are dynamic, characterized in that said supply means (M) include means for executing an algorithm for computing said credentials.

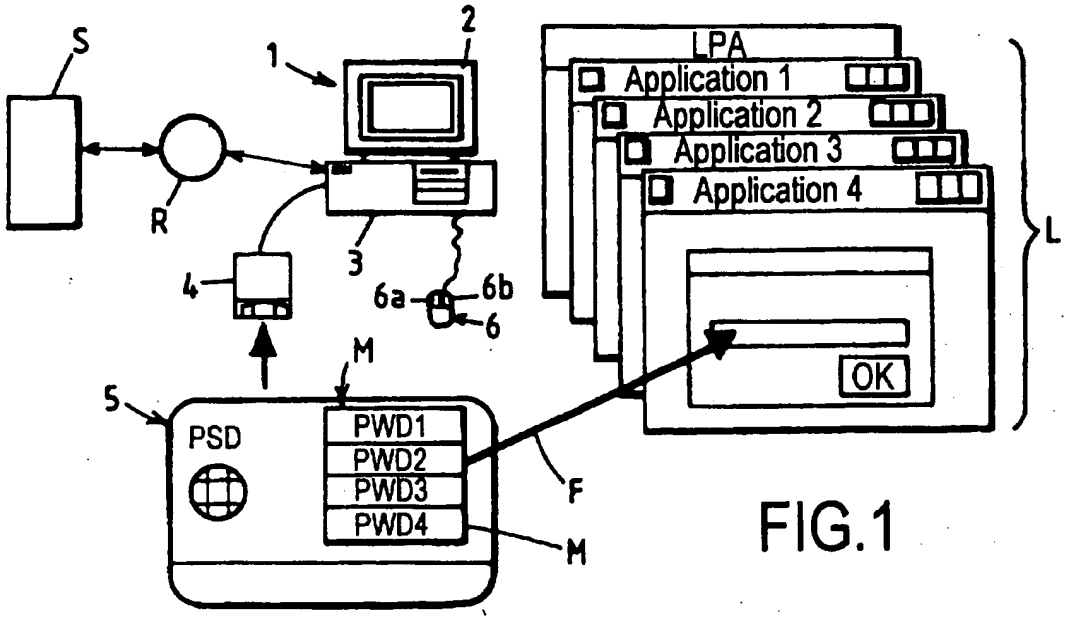
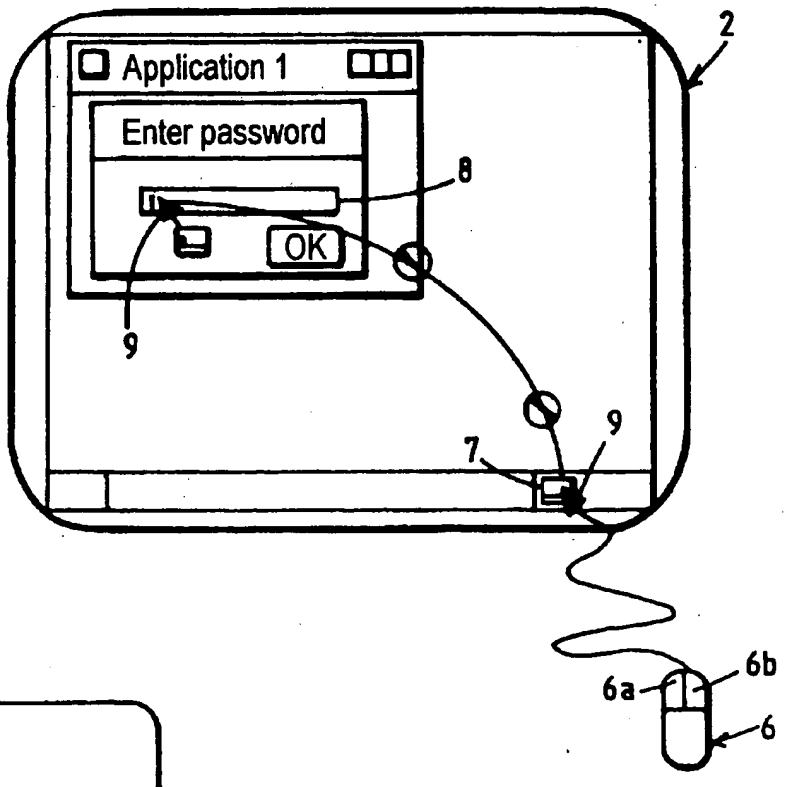


FIG.1

FIG.2A



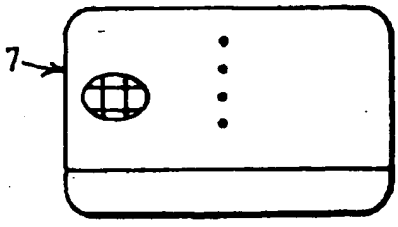


FIG.2B

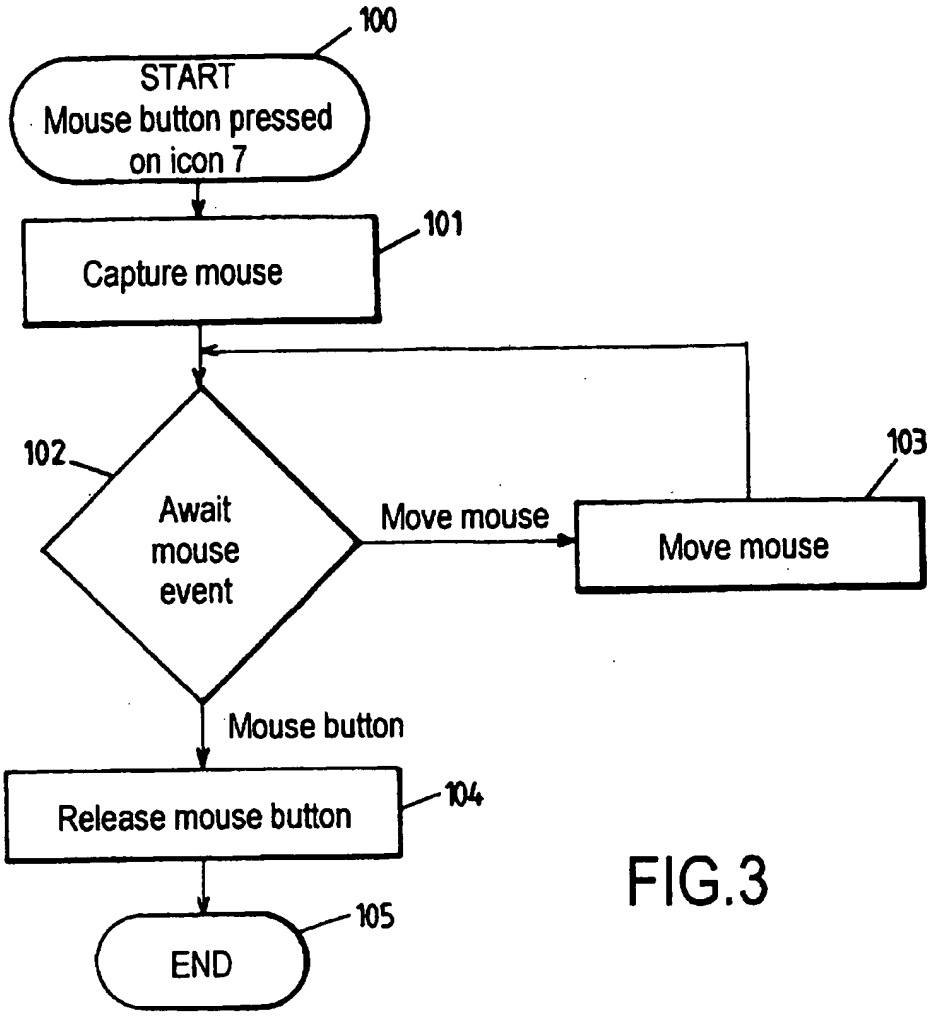

100
START
Mouse button pressed
on icon 7
101
Capture mouse
102
Await
mouse
event
Move mouse
103
Move mouse
Mouse button
Release mouse button
104
105
END

FIG.3

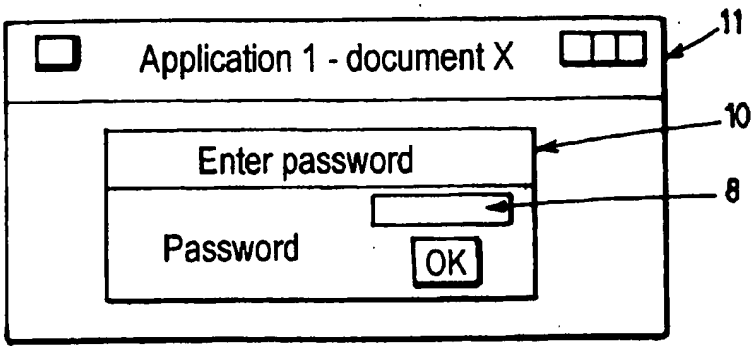

11
Application 1 - document X
10
Enter password
8
Password
OK

FIG.6

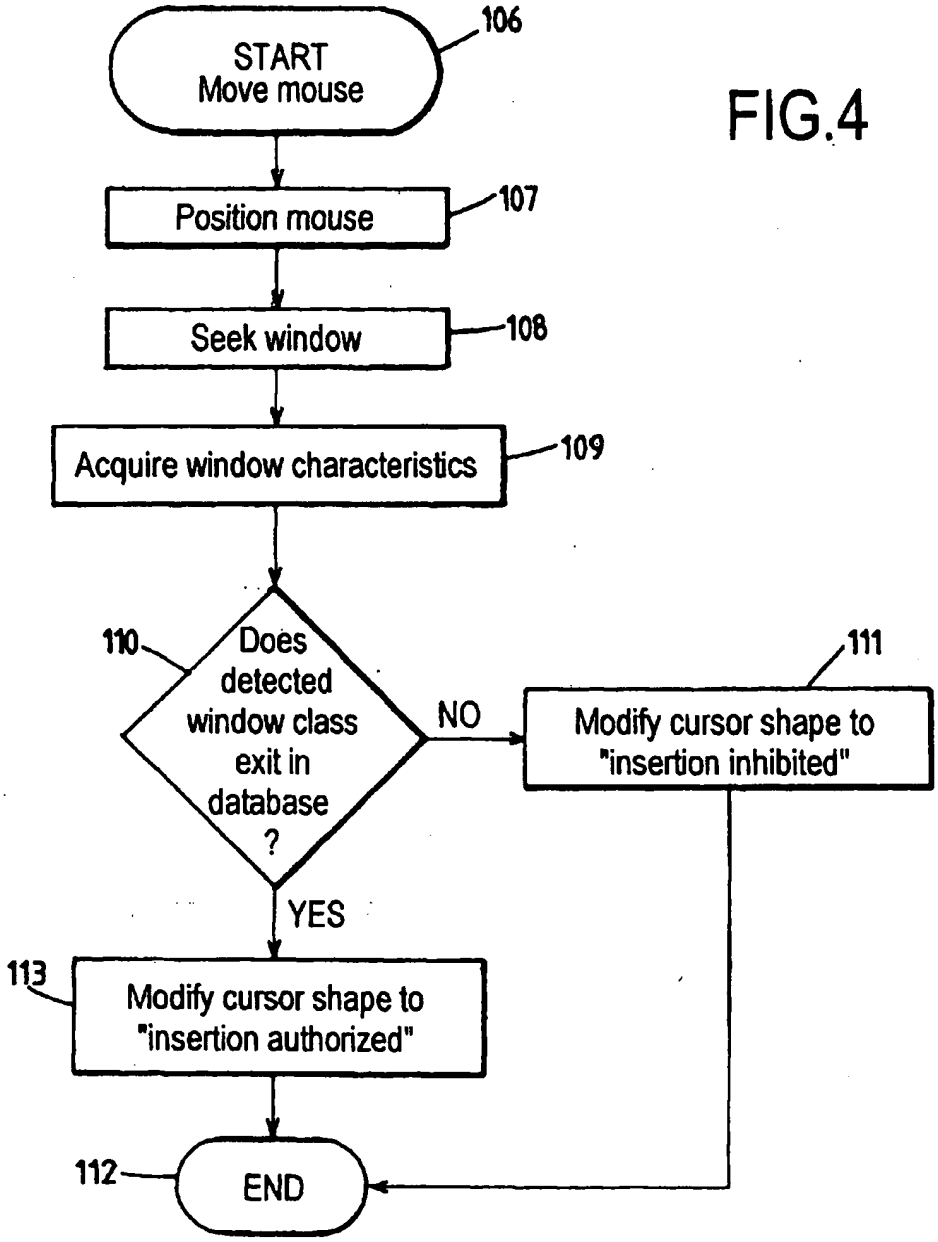

START
Move mouse
106
Position mouse
107
Seek window
108
Acquire window characteristics
109
110
Does detected window class exit in database ?
NO
111
Modify cursor shape to "insertion inhibited"
YES
113
Modify cursor shape to "insertion authorized"
112
END

FIG.4

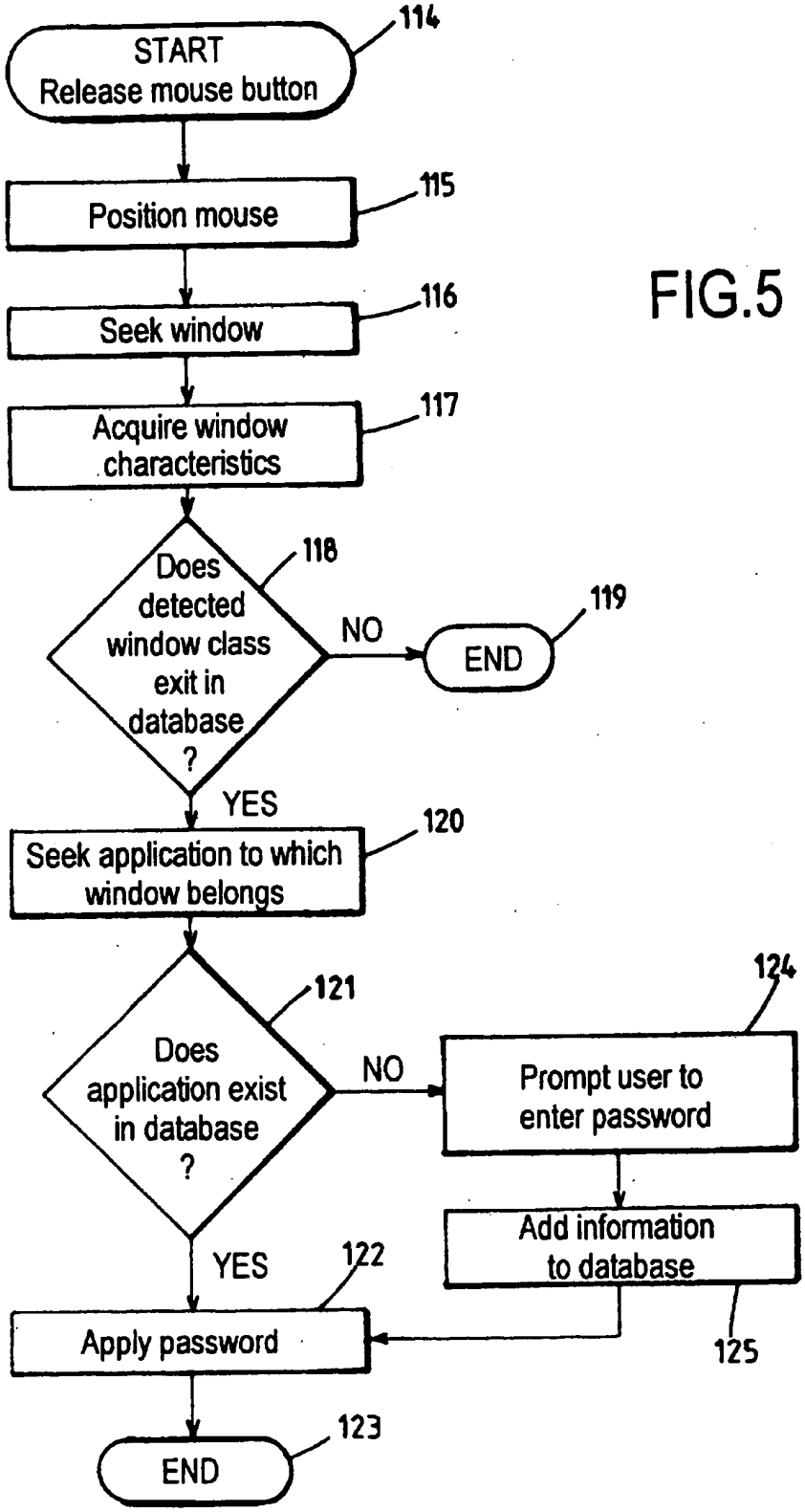

START
Release mouse button
114
Position mouse
115
Seek window
116
Acquire window characteristics
117
Does detected window class exit in database ?
118
NO
END
119
YES
Seek application to which window belongs
120
Does application exist in database ?
121
NO
Prompt user to enter password
124
Add information to database
125
YES
122
Apply password
END
123

FIG.5